UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,518	07/31/2001	Ernest E. Woodward	884.486US1	3616

7590 02/14/2005

Schwegman, Lundberg, Woessner & Kluth, P.A.
P.O. Box 2938
Minneapolis, MN 55402

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/919,518	WOODWARD, ERNEST E.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07312001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 9, the phrase "Blakley-Shamir" is unclear whether it means "Blakley and Shamir" or "Blakley or Shamir;" for the purposes of examination the later will be assumed.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the

> art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 6, 8, 10-17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Downs et al (US 6226618) and further in view of Hardjono (US 6182214).

As per claim 1, Downs et al discloses a method of controlling content usage in a personal communication device using a decryption key, the method comprises: providing the personal communication device a first key in response to a request for content; and verifying credit of a user of the personal communication device; providing the personal communication device a key when the credit is confirmed; for use in decrypting content (see column 9 lines 62-67, and column 10 lines 1-3, 53-63 and column 11 lines 21-24, see also table in columns 18-19).

Downs et al fails to disclose the decryption key being broken into key-shares.

However Hardjono teaches the use of key-shares (see column 3 lines 33-42).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to distribute one of Hardjono's key-shares to each of the servers and users of Downs

et al to be delivered to the use upon request and confirmation of credit.

Motivation to do so would have been to set up a threshold cryptography system (see Hardjono column 3 lines 29-42).

As per claim 2, the modified Downs et al and Hardjono system discloses monitoring usage of the content with a security processor of the personal communications device (see Downs et al column 11 lines 43-48); and purging a key-share when the usage exceeds one of a set of measurement parameters stored in the personal communications device of the set (see Downs et al column 11 lines 43-48 and Hardjono column 3 lines 33-42 where it is clear that if not permitted as described in Downs et al the device would remove a key-share to make the device unable to perform more actions because the key would no longer exist).

As per claim 3, the modified Downs et al and Hardjono system discloses receiving the request for content from the personal communication device, the request identifying the content and the measurement parameters for the content (see Downs et al column 10 lines 53-64).

As per claim 4, the modified Downs et al and Hardjono system discloses receiving the content from a content server in a security server; encrypting the content in the security server with the encryption key and providing the encrypted content from

the security server to the personal communication device over a wireless communication link (see Downs et al column 9 lines 38-43, and column 6 lines 49-56).

As per claim 6, the modified Downs et al and Hardjono system discloses the providing the first of the key-shares is performed by a security server in communication with the personal communication device (see Downs et al column 10 lines 53-63).

As per claim 8, the modified Downs et al and Hardjono system discloses the verifying credit of the user and the providing the second of the key-shares to the personal communication device are performed by a finance server in communication with the personal communication device (see Downs et al columns 18-19).

As per claim 10, the modified Downs et al and Hardjono system discloses the content comprises either video content or music content (see Downs et al column 9 lines 38-40).

As per claim 11, the modified Downs et al and Hardjono system discloses generating a set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit, and wherein the personal communication device monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares

when the usage exceeds one of the measurement parameters of the set (see Downs et al column 9 lines 34-36 and column 10 lines 15-18 and as applied to claim 2).

As per claim 12, the modified Downs et al and Hardjono system discloses a content server defining the set of measurement parameters based on preferences of a content provider (see column 9 lines 15-47).

As per claim 13, the modified Downs et al and Hardjono system discloses the date-limit defines an end calendar date for playing the content, the nm-time limit defines a maximum amount of time for playing portions of the content, and the iteration limit defines a maximum number of times for playing the content or portions thereof (see Downs et al column 10 lines 15-18).

As per claim 14, the modified Downs et al and Hardjono system discloses the measurement parameters have an authentication code associated therewith, and wherein a security processor of the personal communication device purges at least one of the key-shares when the authentication code fails to authenticate (see Downs et al and Hardjono as applied to claim 2 where the authentication code is the watermark).

As per claim 15, the modified Downs et al and Hardjono system discloses the personal communication device receives the

first and second of the key-shares over a wireless communication link (see Downs et al column 6 lines 49-56).

As per claim 16, the modified Downs et al and Hardjono system discloses a security processor portion to combine a plurality of key-shares and decrypt content for the processing system, the security processor portion including a monitor for usage of the content constructed and arranged to purge at least one of the key-shares when the usage exceeds a measurement parameter; and a communications processor portion to receive decrypted content from the security processor portion and providing decrypted content for playing on the personal communication device (see Downs et al column 11 lines 43-48 as applied to claim 2).

As per claim 17, the modified Downs et al and Hardjono system discloses the measurement parameters have an authentication code associated therewith, and wherein a security processor of the personal communication device purges at least one of the key-shares when the authentication code fails to authenticate (see Downs et al and Hardjono as applied to claim 2 where the authentication code is the watermark).

As per claim 19, the modified Downs et al and Hardjono system discloses generating a set of measuring parameters comprising at least one of a date-limit, a run-time limit, and

an iteration limit, and wherein the personal communication device monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters of the set (see Downs et al column 9 lines 34-36 and column 10 lines 15-18 and as applied to claim 2).

As per claim 20, the modified Downs et al and Hardjono system discloses an applications processor portion to process applications running on the personal communication device, and wherein the security processor portion, communications processor portion and applications processor portion are part of a processor area and fabricated on an application specific integrated circuit (ASIC) (see Downs et al Fig. 10).

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Downs et al and Hardjono system as applied to claim 1 above, and further in view of Howard et al (US 20020069365).

As per claim 5, the modified Downs et al and Hardjono system fails to disclose the security server and content server being separate entities.

However, Howard et al teaches a security and content server being separate (see paragraph 68).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the security and content servers of Downs et al and Hardjono to be separate as in Howard et al.

Motivation to do so would be to allow them to be owned by separate people (see Howard et al paragraph 68).

7. Claims 7, 18, 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Downs et al and Hardjono system as applied to claims 1 and 16 above, and further in view of Johnston (US 6373946).

As per claims 7 and 18, the modified Downs et al and Hardjono system fails to disclose receiving a key-share from a SIM.

However, Johnston teaches the use of a SIM to provide a key (see column 9 lines 14-21).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Johnston's SIM to provide one of the key-shares of the modified Downs et al and Hardjono system.

Motivation to do so would have been to make sure the SIM holder has no access and cannot read the key on the SIM (see Johnston column 1 lines 23-38).

As per claim 21, the modified Downs et al, Hardjono and Johnston system discloses a processor area to store first key-share therein (see Downs et al Fig. 10); a module receiving area to receive a subscriber identity module (SIM), the SIM having a second-key share stored therein (see Johnston as applied to claim 18); and an RF interface (see Johnston column 9 lines 14-21) to receive a third key-share and encrypted content over a wireless communication line wherein the processor area includes apparatus constructed and arranged to combine the first, second and third key-shares to decrypt the encrypted content and monitor playing of the decrypted content against measurement parameters (see Downs et al column 11 lines 30-54).

As per claim 22, the modified Downs et al, Hardjono and Johnston system discloses the measurement parameters have an authentication code associated therewith, and wherein a security processor of the personal communication device purges at least one of the key-shares when the authentication code fails to authenticate (see Downs et al and Hardjono as applied to claim 2 where the authentication code is the watermark).

As per claim 23, the modified Downs et al, Hardjono and Johnston system discloses the verifying credit of the user and the providing the second of the key-shares to the personal communication device are performed by a finance server in

communication with the personal communication device (see Downs et al columns 18-19).

8. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Downs et al and Hardjono system as applied to claim 1 above, and further in view of Schneier (Applied Cryptography).

As per claim 9, the modified Downs et al and Hardjono system fails to disclose the key-shares being Blakley-Shamir key shares.

However, Schneier teaches the use of Blakley-Shamir key-shares (see pages 71-72).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's specific key shares as the key shares in the modified Downs et al and Hardjono system.

Motivation to do so would have been the Blakley and Shamir were the inventors of the idea (see Schneier page 72).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bennett et al (US 4864615 A) discloses distributed key generation, Comerford et al (US 5109413 A) discloses a method of deleting keys to

preserve copy protection, Garay et al (US 6192472 B1) discloses a method for using threshold cryptography, Schmeidler et al (US 6763370 B1) discloses secure content distribution, Matsumoto (US 20010013037 A1) discloses a method for distributing encrypted content, and Experton (US 5995965 A) discloses a method for distributing encrypted content.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER